REMARKS/ARGUMENTS

Reexamination of the captioned application is respectfully requested.

A. SUMMARY OF THIS AMENDMENT

By the current amendment, Applicants basically:

1. Editorially amend the specification.
2. Amend claims 1, 5 - 6, 8 - 9, 11, 12, 13 – 15.
3. Add new dependent claims 16 – 20, dependent upon independent claim 8 and corresponding to claims 2 – 6, respectively.
4. Add new dependent claims 21 – 22, dependent upon independent claim 11 and corresponding to claims 9 – 10, respectively.
5. Respectfully traverse all prior art rejections.

B. THE REJECTIONS

Claims 1-2, 5-12 and 14-15 stand rejected under 35 USC 102(a) as being anticipated by WO 01/35613 to Greger et al. Claims 1-2, 5-12 and 14-15 stand rejected under 35 USC 102(a) as being anticipated by WO 00/02361 to Ayoub et al. Claims 4 and 13 stand rejected under 35 USC 103(a) as being unpatentable over WO 00/02361 to Ayoub et al as applied to claims 1-3 above, and further in view of U.S. Publication 2004/0198392 to Harvey et al. Claims 1-2, 5-12 and 14-15 stand rejected under 35 USC 102(e) as being anticipated by U.S. Publication 2004/0175665 to O'Grady et al. Claims 4 and 13 stand rejected under 35 USC 103(a) as being unpatentable over U.S. Publication 2004/0175665 to O'Grady et al as applied to claims 1-3 above, and further in view of U.S. Publication 2004/0198392 to Harvey et al. Claims 1-2, 5-12 and 14-15 stand rejected under 35 USC 102(e) as being anticipated by U.S. Patent 6,243,596 to Kikinis et al. Claims 4 and 13 stand rejected under 35 USC 103(a) as being unpatentable over U.S. Patent 6,243,596 to Kikinis et al as applied to claims 1-3 above, and further in view of U.S. Publication 2004/0198392 to Harvey et al. Claims 1-2, 5-12 and 14-15 stand

rejected under 35 USC 102(e) as being anticipated by U.S. Publication 2002/0013161 to Schaeffer et al. Claims 4 and 13 stand rejected under 35 USC 103(a) as being unpatentable over U.S. Publication 2002/0013161 to Schaeffer et al as applied to claims 1-3 above, and further in view of U.S. Publication 2004/0198392 to Harvey et al. All prior art rejections are respectfully traversed for at least the following reasons.

C. THE REFERENCES

Six applied references are briefly discussed below, as well as DE 10019651 A1 which the Examiner has declined to make of record.

WO 01/35613 A1 to Greger et al. discloses an exchangeable power-supply unit for providing *GPS* and/or Bluetooth functionality as additional functions to a device powered by the power-supply.

US 2004/0198392 A1 to Harvey et al. discloses a high-speed communication link.

WO 00/02361 to Ayoub et al. discloses an exchangeable power-supply unit for providing additional functionality in general to a device powered by the power-supply, *i.e.* in Ayoub there are no or very vague indications of a particular additional function.

US2002/0175665 to O'Grady et al. discloses an exchangeable power-supply unit for providing a media decoder as an additional function to a device powered by the power-supply.

US 6,243,596 B1 to Kikinis et al. discloses an exchangeable power-supply unit for providing an Internet browsing function to a device powered by the power-supply.

US 2002/0013161 A1 to Schaeffer et al. discloses an exchangeable power-supply unit for providing a camera as an additional function to a device powered by the power-supply.

DE 10019651 A1 discloses an exchangeable power-supply unit for providing a GPS as an additional function to a device powered by the power-supply.

From the above it seems clear that none of the six applied references nor DE 10019651 A1 discloses an exchangeable power-supply unit for providing a cryptographic circuit as an additional function to a device powered by the power-supply.

Amended claim 1 and claims dependent thereon are referring thereto are, in fact, directed to an exchangeable power-supplying unit comprising a cryptographic circuit and thus are deemed novel with respect to the foregoing references. Applicants emphasize that there are particular and important problems associated with cryptographic functions that have no counterpart in the solutions presented in foregoing references. For example:

1) The cryptographic function has to be kept secret. Hence, it is important that a cryptographic function can be easily and fully removed when the function is no longer used by the device in question.

2) The correct cryptographic function must be used. Hence, it is important to keep track of the specific cryptographic function to be used. Otherwise encrypted information may be impossible to decrypt and therefore lost.

It follows that the distribution and use of a cryptographic function must be carefully monitored and controlled.[1]

[1] See e.g. page 10 lines 19–27 in the International Application: "The fact that the battery 200 can comprise a small circuit board 220 suitable for production in small series is particularly advantageous in connection with a cryptographic function, since it enables the design of circuit boards comprising a customized cryptographic function that is unique to a small group of users. This strengthens the control and secrecy of the cryptographic hardware and its function. Moreover, the battery 200 may be physically marked with numbers, lines or colors to inform a user whether a cryptographic function is currently in use and if so, the type of cryptographic function that is used etc.", emphasize added.

Known solutions for providing a device with a cryptographic function are based on a key or a software module or similar that is downloaded or otherwise provided to the device, or based on some kind of smart-card or similar that is inserted into the device. Such solutions are afflicted with particular and typical drawbacks, such as the following (listed as non-limiting examples):

- The key/software solutions are "invisible" in that they do not provide any clear indication of the type of cryptographic function being currently used by the device in question. Hence, the risk of using an incorrect cryptographic function is therefore non-negligible. Moreover, the "invisibility" makes it difficult to ascertain whether the cryptographic function has been fully removed when the function is no longer used by the device in question.

- The smart-card solutions are "bulky" in that they require a card receiver in the device, which occupies valuable space and increases the cost. Moreover, smart-card solutions are not "weather proof" since the receiver for a typical smart card is not adapted to be water resistant or otherwise adapted to resist stress from the environment.

The problem of monitoring and controlling the distribution and use of a cryptographic function in devices that are exposed to harsh environment has been known for a long time.[2] However, techniques like the key/software solution and the smart-card solution are unsuitable for these purposes.

[2] C.f. e.g. footnote 1 above, read in conjunction with e.g. page 3 lines 6–12 in the Application: "There is consequently a need for an exchangeable module that provides an additional functionality to a device, which module is large enough to comprise additional hardware needed for the additional functionality, and where the module can be connected to the device to form a compact, highly integrated and small sized apparatus possessing a good protection from the environment. It is also preferred that the module supports a proper modular design so that the device can remain essentially unchanged regardless of the module currently used." , emphasize added.

The foregoing references are completely silent about cryptographic functions and the problem of monitoring and controlling the distribution and use of such functions. The foregoing references do not teach or suggest incorporation of a cryptographic function into a power-supplying unit that is adapted to form an integral and exchangeable part of the device, thereby providing protection from the environment and excellent monitoring of the distribution and use of the cryptographic function by means of *e.g.* visible markings on the power-supplying unit. Rather, the foregoing references are directed to such functions as GPS function, Bluetooth, a media function, Internet browsing or a camera function etc. None of these other functions of the references require any monitoring and control of the distribution and use of the function, as is the case for a cryptographic function. Hence, Applicant submits that the person skilled in the art would not have considered the foregoing references when searching for a solution that improves the control and distribution of a *cryptographic function* in devices that are exposed to harsh environment.

Moreover, even if the skilled person would actually reviewed the foregoing references he or she would not have received any hint from these documents leading to the independent claims. Rather, the skilled person would have taken another track and followed the key/software approach so as to provide a software-based indication of the cryptographic function currently used in the device, e.g. a software solution that provides an indication on a display or similar comprised by the device. This would have improved the control and distribution of the cryptographic function compared to the invisibility of the key/software approach mentioned above and it would not have exposed the interior of the device to the environment.

Therefore, it is respectfully submitted that Applicants' independent claims are novel and patentable.

D. **MISCELLANEOUS**

In view of the foregoing and other considerations, all claims are deemed in condition for allowance. A formal indication of allowability is earnestly ted.

The Commissioner is authorized to charge the undersigned's deposit account #14-1140 in whatever amount is necessary for entry of these papers and the continued pendency of the captioned application.

Should the Examiner feel that an interview with the undersigned would facilitate allowance of this application, the Examiner is encouraged to contact the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /H. Warren Burnam, Jr./

H. Warren Burnam, Jr.
Reg. No. 29,366

HWB:lsh
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100